ETSI TR 133 927 V18.2.0 (2024-05)

TECHNICAL REPORT

5G;
Security Assurance Specification (SCAS);
threats and critical assets in 3GPP virtualized network product classes
(3GPP TR 33.927 version 18.2.0 Release 18)

Reference

DTR/TSGS-0333927vi20

Keywords

5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document captures the virtualized network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The present document contains generic aspects that are believed to apply to more than one network product class. In another aspect, present document defines different types of virtualized network products compared to only one type defined in [2].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[3] 3GPP TR 33.936: "Security Assurance Methodology (SECAM) for 3GPP virtualized network products".

[4] 3GPP TR 23.501: " System architecture for the 5G System (5GS) Stage 2".

[5] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[6] ETSI GS NFV-EVE 001: "Network Functions Virtualisation (NFV); Virtualisation technologies; Hypervisor Domain Requirements Specification".

[7] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

[8] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; VNF Descriptor and Packaging Specification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

EM	Element Management
GVNP	Generic Virtualized Network Product
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	Network Functions Virtualization Orchestrator
OAM	Operation and Management
SCAS	Security Assurance Specification
VIM	Virtualized Infrastructure Manager
VM	Virtual Machine
VNFM	Virtualized Network Function Manager

4 Generic Virtualized Network Product (GVNP) class description

4.1 Overview

A 3GPP generic virtualized network product class defines a set of functions that are implemented on that product, which includes, but not limited to minimum set of common 3GPP functions for that product covered in 3GPP specifications, other functions and softwares not covered by 3GPP specifications, as well as interfaces to access that product. A generic type 1 of virtualized network product may also include software, and OS components that the product is implemented on. The present document describes the threats and the critical assets in the course of developing 3GPP security assurance specifications for a particular network product class.

NOTE: Considering the situation that type 2 and/or type 3 of virtualized product class are dependent of pre-mature specifications from other standard organization, only type 1 of virtualized product class are specified in present document.

Applicability of the GVNP security assurance specification to products: Assume a telecom equipment vendor wants to sell a product to an operator, and the latter is interested in following the Security Assurance Methodology as described in TR 33.936 [3], then, before evaluation according to TR 33.936 [3] in a testing laboratory can start, it first needs to be determined which security assurance specifications written by 3GPP apply to the given product.

Different with 3GPP GNP defined in TR 33.926 [2], based on different implementation, 3GPP VNP will be categorized as 3 types. As a result, a type 1 of 3GPP Virtualized Network Product may be composed with software (e.g. operating system, drivers, applications, services, protocols), and interfaces (e.g. console interfaces and O&M interfaces) that allow the 3GPP network product to be managed and configured locally and/or remotely. A GVNP is a 3GPP network product.

GVNP Security Assurance Specification (GVNP SCAS): The GVNP SCAS provides descriptions of the security requirements (which are including test cases) pertaining to type 1 of generic virtualized network product class.

Need for a GVNP network product model: This minimum set of functions listed in clause 4.2 is exclusively meant as a membership criterion for the GVNP Class. It is not meant to restrict the functionality of a GVNP, nor the scope of the present document in any way. On the contrary, it is clear that GVNPs will contain many more functions than those from the minimum set listed in clause 4.2, and the GVNP will contain requirements relating to functions not contained in this minimum set. Some of these functions, beyond the minimum set, can be found from various 3GPP specifications, but by far not all these functions. This implies that there is a need to describe the functions that cannot be found from 3GPP specifications in some other way before the GVNP can be written so that the GVNPs can make reference to this description. This description is the GVNP model, cf. clause 4.3.

EXAMPLE 1: 3GPP specifications do not describe a local management interface, but GVNPs will have to take it into account, so a local management interface needs to be part of a GVNP model.

EXAMPLE 2: A GVNP sometimes says e.g.: "Authentication events on the local management interface shall be logged." This implies the presence of a logging function. The logging function is not part of the defining minimum set of functions from clause 4.2. If a product implements this minimum set, but no logging function, then this just means that the product is a GVNP, but will fail the evaluation against the GVNP SCAS.

The GVNP models are further used in clauses 5 and 6 in various ways, e.g. the critical assets can point to parts of the GVNP model, threats and requirements can refer to interfaces shown in the GVNP model, etc.

4.2 Minimum set of functions defining the GNP class

According to TR 33.936 [3], a virtualized network product class is a class of products that all implement a common set of 3GPP-defined functionalities. This common set is defined to be the list of functions contained in pertinent 3GPP specifications, such as clause 5 of TS 23.501 [4].

4.3 Generic virtualized network product model

4.3.1 Introduction

A virtualized network product class is the class of products that implement 3GPP defined network functionalities running on Network Function Virtualization Infrastructure (NFVI). The realistic deployment scenarios are summarized in ETSI NFV-SEC 001 [7], based on which a 3GPP network operator can deploy 3GPP defined functionalities in three modes:

- Mode 1. A network operator purchases 3GPP VNFs from its vendors and deploys it on a third party NFVI.
- Mode 2. A network operator purchases 3GPP VNFs and the Virtualization layer (e.g. hypervisor) from its vendors, and deploys them on a third party hardware layer.
- Mode 3. A network operator purchases and deploys 3GPP VNFs, the Virtualization layer and the hardware layer from its vendors.

NOTE 1: In order to implement virtualized product, some essential components besides 3GPP defined functions are also needed.

As a result, it defines type 1 of GVNP which is implement 3GPP defined functionalities only.

NOTE 2: Considering the situation that type 2 and/or type 3 of virtualized product class are dependent of pre-mature specifications from other standard organization, only type 1 of virtualized product class are specified in present document.

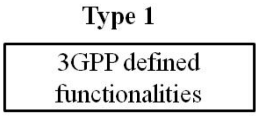

Figure 4.3-1: Type 1 of virtualised network product class

The rest part of device could be seen as a supporting environment and is not considered in scope of those types.

NOTE 3: For the purpose of testing a 3GPP GVNP of type 1, NFVI for GVNP for type 1 are assumed to have gone through security assurance testing in the same rigorous manner that is similarly applied to the security assurance testing of any other 3GPP network product under consideration in SCAS.

The generic virtualized network product model classes are described in the following clauses.

4.3.2 Generic virtualized network product model of type 1

4.3.2.1 Description of the GVNP model

For the virtualized network product class type 1 (i.e. implementing 3GPP defined functionalities only), the following figure 4.3-2 depicts the components of a generic virtualized network product model at a high level.

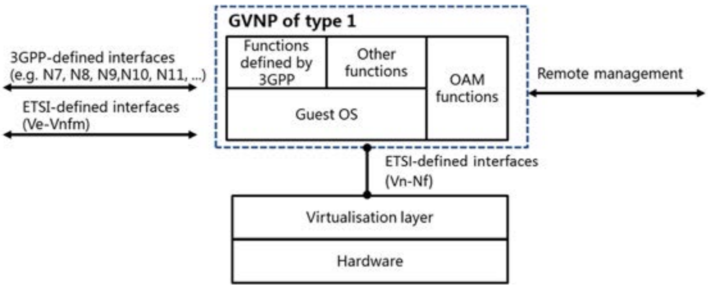
GVNP of type 1
Functions defined by 3GPP
Other functions
OAM functions
Guest OS
3GPP-defined interfaces (e.g. N7, N8, N9,N10, N11, ...)
ETSI-defined interfaces (Ve-Vnfm)
Remote management
ETSI-defined interfaces (Vn-Nf)
Virtualisation layer
Hardware

Figure 4.3-2: GVNP model of type 1

The components in the figure 4.3-2 are further described in the following clauses.

4.3.2.2 Functions defined by 3GPP

For a generic virtualized network function, it will implement 3GPP-defined functions. Unlike a generic physical network product defined in [2], a 3GPP-denfined function can be deployed in multiple VMs and the feature s supported in different VM of the GVNP are up to the implementation of vendors.

To maintain generality and avoid overlap, the GVNP SCAS intends to explicitly address all GVNP functions that, if present in a GVNP, need to be evaluated and hence covered by the requirements in the GVNP SCAS.

4.3.2.3 Other functions

A GVNP will also contain functionalities not or not fully covered in 3GPP specifications.

Examples include, but are not limited to, remote management functions.

4.3.2.4 Operating system (OS)

The present document assumes that the functions of GVNP are implemented on multiple VMs. Each VM which is running on a common platform requires a guest operating system to run.

4.3.2.5 Interfaces

Compared to generic physical network product defined in [2], GVNP has also two types of logical interfaces, i.e. execution environment interfaces and remote logical interfaces.

The remote logical interfaces are interfaces which can be used to communicate with the GVNP from another network node and also include the remote access interfaces to the GVNP for its maintenance through e.g. an Element Management (EM), a Virtualized Network Function Manager (VNFM).

A GVNP hosts the following remote logical interfaces:

- Service interfaces that are defined in pertinent 3GPP specifications

- Service interfaces that are not defined by 3GPP- Access interfaces to the GNP for its maintenance through e.g. an Element Management System (EMS) or other management functions, e.g. remote OAM interface, interface between EM (Element Management) and VNF which proprietary interface (see figure 4.3-3).
- Interface defined by ETSI NFV specifications [5] and [6]:
    - Interface between VNF and VNFM for GVNP lifecycle management, configuration information exchange, state information exchange necessary for network service lifecycle management, etc. This interface refers to Ve-Vnfm in the figure 4.3-3.
    - An execution environment interface is an interface that can be used to provide the GVNP with the underlying execution environment, to guarantee hardware independent lifecycle, portability, and performance requirements of the GVNP. A GVNP type 1 hosts the following execution environment interface:
- Interface towards the underlying Virtualization layer for execution environment provision. This interface refers to Vn-Nf in the figure 4.3-3.

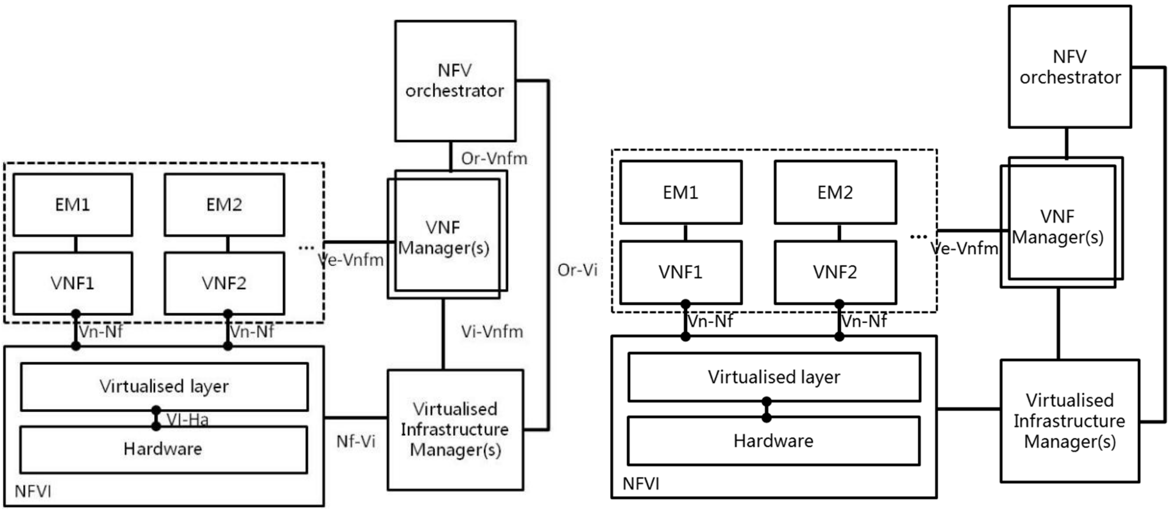

Figure 4.3-3: NFV reference architectural framework

4.4 Scope of the present document

4.4.1 Introduction

The present subclause refers to the GVNP model in clause 4.3.

4.4.2 Scope regarding GVNP functions defined by 3GPP

The set of functions implemented in network products as described in TR33.926 [2] applies to the corresponding GVNP.

The GVNP SCAS needs to explicitly address all GVNP functions that, if present in a GVNP network product, need to be evaluated and hence covered by requirements in the GVNP SCAS. The GVNP SCAS should not be tied to a specific version

4.4.3 Scope regarding other functions

At least the following functions, that are not defined by 3GPP, are in scope of the GVNP SCAS:

- Remote management functions
- Local management functions

4.4.4 Scope regarding Operating System (OS)

The GVNP SCAS does not attempt a full evaluation of the correct internal functioning of guest OS. However, interfaces (i.e. the restriction on open ports and unnecessary services running in the system) and modifications (e.g. verification of the correct applied patch level, hardening, etc.) of the OS are in scope.

4.4.5 Scope regarding hardware

Hardware is not included based on the type 1 model of GVNP SCAS. As a result, hardware is not in scope of for the type 1 of GVNP SCAS.

4.4.6 Scope regarding interfaces

The interfaces listed in clause 4.3.2.5 are all in scope of the present document.

5 Generic assets and threats

5.1 Introduction

The present subclause contains assets and threats that are believed to apply to more than one virtualized network product.

5.2 Critical assets

5.2.1 Generic assets of GVNP for type 1

The critical assets of GVNP for type 1 that need to be protected are:

- User account data and credentials (e.g. passwords, private key);
- Log data;
- Configuration data, e.g. GVNP's IP address, ports, VPN ID, Management Objects (e.g. user group, command group) etc.;
- Guest Operating System, i.e. the files that make up the guest OS and its processes (code and data);
- GVNP Application;
- Sufficient processing capacity: that processing powers are not consumed close to limits;
- The interfaces of GVNP to be protected and which are within SECAM scope: for example:
    - OAM interface, for remote access: interface between GVNP and OAM system;
    - Interface between virtualised network function (VNF) and VNFM;
    - Interface between VNF and virtualisation layer, for providing the execution environment to run VNF;
- GVNP Software package (binary code or executable code) which includes:
    - VNFD;
    - VNF image and image description file;
    - Configuration data (e.g. manifest file as defined in [8]).

5.3 Threats

5.3.1 Generic threats format

Threats are described using the following format:

- Threat Name:
- Threat Category:
- Threat Description:
- Threatened Asset:

5.3.2 Generic threats for GVNP of type 1

5.3.2.1 Introduction

In clause 5.3.1 of TR 33.926 [2], the identified threats are grouped into seven categories, one covering threats relating to 3GPP-defined interfaces and the other six corresponding to the categories proposed by STRIDE. Since these seven categories are for generic 3GPP network products, they are also applicable to GVNP of type 1. In addition, GVNP of type 1 also needs to consider the threats related to ETSI-defined interfaces. As a result, there are eight categories of threats for GVPN of type 1. The following clauses describe the threats according to these security categories and use the template of threat description in clause 5.3.1 of TR 33.926 [2]. For threats descriptions of current seven categories, the present document will focus on the differences between GVNP threats and GNP threats which are described in TR 33.926 [2].

5.3.2.2 Threats relating to 3GPP-defined interfaces

For GVNP of type1 and GNP in TR 33.926 [2], the threats related to 3GPP-defined interfaces are the same. So, all texts in clause 5.3.2 of TR 33.926 [2] apply to GVNP of type 1. It means that there is no need repeat the threats relating to 3GPP-defined interfaces which are covered in 3GPP security specifications. If threats relating to 3GPP-defined interfaces are found not sufficiently covered in existing 3GPP security specifications, they need to be addressed in the SCAS for virtualised network products.

5.3.2.3 Threats relating to ETSI-defined interfaces

Two of the interfaces defined in ETSI NFV specification [5] are identified as the critical assets of GVNP type 1, i.e. interface between VNF and VNFM, interface between 3GPP VNF and virtualisation layer. The threats on these interfaces are as follows.

- Threats on interface between 3GPP VNF and VNFM: if the interface is not protected, an attacker can attack all the requests/responses sent between the VNF and the VNFM. For example, the attacker can insert, tamper or delete e.g. scaling requests, healing requests, subscribe requests, query requests and other management related requests sent from the instantiated GVNP of type 1 to the VNFM, hence the virtualised resource or relevant status information obtained by the instantiated GVNP of type 1 is not as requested. This affects the normal operation of the instantiated GVNP of type 1, and even causes DoS attacks, information leakage.

NOTE: The Virtualisation layer is out of 3GPP scope, but its protection will affect the security of the upper layer it supports. If the Virtualisation layer is compromised, the VNF on top of it could also be easily compromised. In such case, the messages sent over the VNF-VNFM interface can be manipulated by the compromised VNF, which is however not a threat coming from the VNF-VNFM interface. The analysis above focuses on the threats directly placed on VNF-VNFM interface, when it is not well protected.

- Threats on interface between 3GPP VNF and virtualisation layer: an attacker can attack an instantiated GVNP of type 1 through a compromised virtualisation layer. For example, cryptographic keys or other security critical data of an instantiated GVNP of type 1 could be stolen by an attacker with access to the virtualisation layer, or the virtualised resource provided by the Virtualisation layer to the instantiated GVNP of type 1 can be manipulated or the bootloader of Guest OS of an instantiated GVNP of type 1 can be tampered by an attacker via a compromised virtualisation layer.

5.3.2.4 Spoofing identity

5.3.2.4.1 Default Accounts

The threat in clause 5.3.3.1 of TR 33.926 [2] applies to GVNP of type 1.

The difference is that VNF is accessed through VNC (Virtual Network Console) rather than through the physical console interface, an attacker can use a default account to access a VNF via VNC.

5.3.2.4.2 Weak Password Policies

The threat in clause 5.3.3.2 of TR 33.926 [2] applies to GVNP.

However, the attacker using the weak password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.3.2.4.3 Password peek

The threat in clause 5.3.3.3 of TR 33.926 applies to GVNP.

However, the attacker using the peeked password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.3.2.4.4 Direct Root Access

The threat in clause 5.3.3.4 of TR 33.926 [2] applies to GVNP of type 1.

There are no differences between direct root accesses for GVNP and GNP described in TR 33.926 [2].

5.3.2.4.5 IP Spoofing

The threat in clause 5.3.3.5 of TR 33.926 [2] applies to GVNP of type 1.

However, the objective of unauthorized access is a VNF, not a computer.

5.3.2.4.6 Malware

The threat in clause 5.3.3.6 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.4.7 Eavesdropping

The threat in clause 5.3.3.7 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.5 Tampering

5.3.2.5.1 Software Tampering

The threat in clause 5.3.4.1 of TR 33.926 [2] applies to GVNP of type 1.

Different from traditional physical network products, as the entire GVNP is instantiated by the image(s) and other information (e.g. configuration data, software environmental parameters, licence terms information, script, manifest file, checksum, etc. as defined in [8]) within a software package, additional threats are analysed as follows:

- *Threat Name*: Software Tampering
- *Threat Category*: Tampering

- *Threat Description*: Compared with GNP software, GVNP software has additional attack surfaces, e.g. in the process of VNF package on boarding, during which the software package of a GVNP can be tampered/altered if not protected. An attacker, for example, can inject malicious code or tamper the information inside the unprotected package during on boarding. Then after the instantiation of the GVNP, the tampered code can be executed to conduct several attacks (e.g. DoS, Information Stealing, Frauds and so on).

- *Threatened Asset*: all critical assets of GVNP type 1 as listed in clause 5.2.1.

5.3.2.5.2 Ownership File Misuse

The threat in clause 5.3.4.2 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.5.3 Boot tampering for GVNP of type 1

For GVNP of type 1, there is no hardware. This is different from external device boot of GNP described in clause 5.3.4.3 of TR 33.926 [2]. The threat is described as follows:

- *Threat name*: GVNP of type 1 boot tampering

- *Threat Category*: Tampering

- *Threat Description:* the GVNP bootloader may be maliciously tampered by an attacker, e.g. the attacker tampers the bootloader of GVNP through a malicious virtualisation layer.

- *Threatened Asset:* guest operating system

5.3.2.5.4 Log Tampering

The threat in clause 5.3.4.4 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.5.5 OAM traffic Tampering

The threat in clause 5.3.4.5 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.5.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.5.7 User Session Tampering

The threat in clause 5.3.4.7 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.6 Repudiation

5.3.2.6.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7 Information disclosure

5.3.2.7.1 Poor key generation

The threat in clause 5.3.6.1 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.2 Poor key management

The threat in clause 5.3.6.2 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.3 Weak cryptographic algorithms

The threat in clause 5.3.6.3 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.4 Insecure Data Storage

- *Threat name*: Insecure Data Storage
- *Threat Category*: Information Disclosure
- *Threat Description:* The GVNP remotely stores sensitive data (e.g. passwords, private keys, logs) on the logical volume that the VIM allocates to the GVNP. An attacker can retrieve these data if they have been stored in an insecure way (e.g. clear text, unsalted hashes).
- *Threatened Asset*: Any sensitive data stored on the logical volume of the GVNP

5.3.2.7.5 System Fingerprinting

The threat in clause 5.3.6.5 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.6 Malware

- Threat name: Malware.
- Threat Category: Information Disclosure.
- Threat Description: A malware installed on the logical volume that the VIM allocates to the GVNP can access to the stored sensitive data (e.g. subscription data, logs).
- Threatened Asset: Any sensitive data stored on the logical volume of the GVNP.

5.3.2.7.7 Personal Identification Information Violation

The threat in clause 5.3.6.7 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.8 Insecure Default Configuration

The threat in clause 5.3.6.8 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.9 File/Directory Read Permissions Misuse

The threat in clause 5.3.6.9 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.10 Insecure Network Services

The threat in clause 5.3.6.10 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.11 Unnecessary Services

The threat in clause 5.3.6.11 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.12 Log Disclosure

The threat in clause 5.3.6.12 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.13 Unnecessary Applications

The threat in clause 5.3.6.13 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.14 Eavesdropping

The threat in clause 5.3.6.14 of TR 33.926 [2] applies to GVNP of type 1.

5.3.2.7.15 Security threat caused by lack of GVNP traffic isolation

The threat in clause 5.3.6.15 of TR 33.926 [2] applies to GVNP of type 1.

Different from traditional physical network products, as GVNP provides abundant computing, storage and network resources for users. With Virtualization, traditional physical network security appliances can not be used to secure virtual networks between VM on the same physical server. Additional threats are analysed as follows:

- *Threat name*: Security threat caused by lack of GVNP traffic isolation.
- *Threat Category*: Information Disclosure.
- *Threat Description*: Virtual network has invisible traffic between VMs on the same physical server, which is not protected by the traditional network security monitoring means. Flaws such as incomplete isolation of virtual machine resources and the difficulty of monitoring traffic between virtual machines can lead to unauthorized access to VMs and mutual attacks between VMs.
- *Threatened Asset*:Any sensitive data in transit between VMs on the same physical server.

5.3.2.8 Denial of Service

The threats in all clauses of clause 5.3.7 for TR 33.926 [2] apply to GVNP of type 1.

In addition, there is DoS attack due to changing virtualisation resource that is used by GVNP. The detailed threat description is as follows:

- *Threat name*: changing virtualisation resource without authorization.
- *Threat Category*: DoS.
- *Threat Description*: There are several ways to cause a DoS attack for the GVNP: attackers having access to a compromised virtualisation layer can change the virtualisation resource used by the instantiated GVNP of type1 without authorization, or a malicious VM deployed for one instance of a VNF on a host can illegally occupy the resources of the instantiated GVNP of type1 deployed on the same host, resulting in resource limitation of the instantiated GVNP of type1, or attackers having access to a compromised VNFM can scale in a Type 1 or scale down the virtualisation resource used by a GVNP or even terminate a Type 1 instance without authorization.
- *Threatened Asset*: GVNP applications, sufficient processing capacity.

5.3.2.9 Elevation of privilege

The threats in all clauses of clause 5.3.8 for TR 33.926 [2] apply to GVNP of type 1.

6 Generic assets and threats for network functions supporting SBA interfaces

The assets and threats for virtualized network functions supporting SBA interface are the same as the assets and threats specified in clause 6 for TR 33.926 [2].

Annex A:
Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2023-03	SA#99	SP-230130				Presented for information and approval	1.0.0
2023-03	SA#99					Upgrade to change control version	18.0.0
2023-03	SA#99					EditHelp review	18.0.1
2023-12	SA#102	SP-231346	0001		F	Clarification EMS interface to align with TR 33.926	18.1.0
2024-03	SA#103	SP-240374	0002	1	F	Add VM traffic isolation security threat to TR 33.927 3GPP virtualized network product classes	18.2.0

History

Document history		
V18.2.0	May 2024	Publication